LOCALIC GALOIS THEORY

EDUARDO J. DUBUC

ABSTRACT. In this article we prove the following:

A topos with a point is connected atomic if and only if it is the classifying topos of a localic group, and this group can be taken to be the locale of automorphisms of the point.

We explain and give the necessary definitions to understand this statement.

The hard direction in this equivalence was first proved in print in [4], Theorem 1, Section 3, Chapter VIII, and it follows from a characterization of atomic topoi in terms of open maps and from a theory of descent for morphisms of topoi and locales.

We develop our version and our proof of this theorem, which is completely independent of descent theory and of any other result in [4]. Here the theorem follows as an straightforward consequence of a direct generalization of the fundamental theorem of Galois.

In Proposition I of "Memoire sur les conditions de resolubilite des equations par radicaux", Galois established that any intermediate extension of the splitting field of a polynomial with rational coefficients is the fixed field of its galois group. We first state and prove the (dual) categorical interpretation of of this statement, which is a theorem about atomic sites with a *representable* point. These developments correspond exactly to *Classical Galois Theory*.

In the general case, the point determines a proobject and it becomes (tautologically) prorepresentable. We state and prove the, mutatus mutatis, prorepresentable version of Galois theorem. In this case the *classical* group of automorphisms has to be replaced by the *localic* group of automorphisms. These developments form the content of a theory that we call *Localic Galois Theory*.

INTRODUCTION

In this article we prove the following:

Theorem B: A topos $\mathcal{E}$ with a point $\mathcal{E}ns \xrightarrow{p} \mathcal{E}$, $p^* = F$, is connected atomic if and only if it is the classifying topos $\mathcal{B}G$ of a localic group G, and this group can be taken to be $lAut(F) = lAut(p)^{op}$.

We shall explain and give the necessary definitions to understand this statement.

The hard direction in this equivalence was first proved in print in [4], Theorem 1, Section 3, Chapter VIII, and it follows from the characterization of atomic topoi as those topoi such that $\mathcal{E} \to \mathcal{E}ns$ and

the diagonal $\mathcal{E} \xrightarrow{\Delta} \mathcal{E} \times \mathcal{E}$ are open, and from a theory of descent for morphisms of topoi and locales.

We develop our version and our proof of this theorem, which is completely independent of descent theory and of any other result in [4]. Here the theorem follows as an straightforward consequence of a direct generalization of the fundamental theorem of Galois.

In Proposition I of "Memoire sur les conditions de resolubilite des equations par radicaux", (see [3]), Galois established that any intermediate extension of the splitting field A of a polynomial with rational coefficients is the fixed field of its galois group. We first state and prove the (dual) categorical interpretation (Theorem 1.3 below) of of this statement (in the dual category the fixed field is the quotient of A by the action of the galois group). This interpretation is a theorem about atomic sites. From this result (1.3) it follows in an straightforward manner the following:

Theorem A: A topos $\mathcal{E}$ with a representable point $\mathcal{E}ns \xrightarrow{p} \mathcal{E}$, $p^* = [A, \,-]$, $A \in \mathcal{E}$ is connected atomic if and only if it is the classifying topos $\mathcal{B}G$ of a discrete group G, and this group can be taken to be $Aut(A)^{op}$.

We call this development the *representable case* of Galois Theory, and it corresponds exactly to *Classical Galois Theory*.

In the general case, the point p^* determines a proobject P and it becomes (tautologically) prorepresentable $p^* = [P, \,-]$. Theorem 2.3 below is just the prorepresentable version of Theorem 1.3. In this case the classical group of automorphisms $Aut(P)$ has to be replaced by the localic group $lAut(P)$ (whose points form the group $Aut(P)$ which can be trivial). Theorem B follows from this result (2.3) in the same straightforward manner than Theorem A from 1.3.

We call this development the *prorepresentable case* of Galois Theory, and it is the content of a theory that we call *Localic Galois Theory*.

A *localic space* is the formal dual of a local, and a *localic group* is a group object in the category of localic spaces.

Our basic approach is to work with locales, and consider them as posets (as in topos theory one works with topoi as categories). After all, one can hardly expect to prove all the results about localic spaces which are false for topological spaces if one works "as if they were topological spaces" (arguments justified by test maps and the like). It is some times surprising how localic techniques are very often more simple and clear than its dual geometrical counterparts. Geometrical intuition and experience is important to an overall understanding, but when it comes to prove basic results it is of little help (however it is useful, as in topos theory, in order to develop implication chains utilizing basic results).

This paper is divided in eight short sections, with the principal contributions in sections 2., 4. and 6.

In section 1 we state and prove our interpretation of the theorems of classical Galois Theory, (theorems 1.2 and 1.3), and then we prove theorem A in the introduction.

In section 2 we state explicitly the theorems of localic Galois Theory (theorems 2.2 and 2.3).

In section 3 we fix the terminology and notation on locales, and recall some necessary facts.

In section 4 we develop a fundamental construction in this paper, namely, that of the localic group $lAut(F)$ of automorphisms of a set valued functor $\mathcal{C} \xrightarrow{F} \mathcal{E}ns$. To prove theorems 2.2 and 2.3 the straightforward construction, as the appropriate subspace of the product $\prod_{X \in \mathcal{C}} lAut(FX)$, is useless.

Unlike the locale $lAut(X)$ of automorphisms of a set X, the locale of relations $lRel(X)$ is functorial on X, with values in the category of Posets. This is technically of great importance, since it allows to develop constructions corresponding to Grothendieck's construction of the (co)-fibered category associated to a functor with values in the category of Categories. We exploit this in our construction of the locale $lAut(F)$, for a set valued functor F, *by first constructing the locale* $lRel(F)$, and then the locale (subspace) of 2-valued sheaves for the Grothendieck topology that forces a relation to be a bijection. We were inspired by Gavin Wraith presentation in [5] of the locale of automorphisms of a set X.

Section 5 is technical on the generation of grothendieck topologies out of some basic covers.

Section 6 (together with section 4) contains the important contributions made in this paper. Here we prove the fundamental theorems of localic Galois theory. That is, the theorems of section 2 on the prorepresentable case (theorems 2.2 and 2.3).

In section 7 we recall several necessary facts on the category of sets furnished with a continuous action of a localic group. Although this facts are widely believed to be true, nobody has cared to prove them in print.

Finally, in section 8 we show how theorem B follow from the theorems in section 2.

1. Classical Galois Theory

This corresponds to the representable case of the theory. Notice that in the category dual of the category of intermediate extensions of the splitting field A of a polynomial with rational coefficients, the fixed field of a group $H \subset Aut(A)$ is, categorically, the quotient of A by the action of H.

Let $\mathcal{C}$ be any category and $A \in \mathcal{C}$ be any object. Assume:

Assumption 1.1.
   i) Every arrow $Y \longrightarrow X$ in $\mathcal{C}$ is an strict epimorphism.
   ii) For every $X \in \mathcal{C}$ there exists $A \longrightarrow X$.
   iii) The representable functor $F = [A, -]$ preserves strict epimorphisms.

Then:

Theorem 1.2. *For every object $X \in \mathcal{C}$ the action of the group $Aut(A)^{op}$ on the set $[A, X]$ is transitive.*

Theorem 1.3 (Galois Theorem). *Every arrow $A \xrightarrow{x} X$ in $\mathcal{C}$ is the categorical quotient of A by the action of the Galois group $Fix(x) = \{h \in Aut(A) \mid xh = x\} \subset Aut(A)$.*

These theorems follow easily from the following proposition:

Proposition 1.4. *Every arrow $X \xrightarrow{f} A$ is an isomorphism. In particular, every endomorphism of A is an isomorphism, $Aut(A) = [A, A]$.*

Proof. In fact, from iii) it follows that there is $A \xrightarrow{g} X$ such that $fg = id$. Then, g is a monomorphism. Since by i) it is also an strict epimorphism, it follows that it is an isomorphism, and consequently so is f.   □

Proof of theorems 1.2 and 1.3

Proof. Theorem 1.2 follows immediately from iii). Let now $A \xrightarrow{x} X$, and assume $A \xrightarrow{y} Y$ is any arrow such that $Fix(x) \subset Fix(y)$. Since x is an strict epimorphism (see 6.1), to prove theorem 1.3 it will be

enough to show that given any two arrows $Z \underset{s}{\overset{t}{\rightrightarrows}} A$, the implication

"$xs = xt \implies ys = yt$" holds. By 1.4 we can assume $Z = A$ and s invertible. Let $xs = xt$, then $ts^{-1} \in Fix(x)$, thus also $ts^{-1} \in Fix(y)$. Thus $ys = yt$. $\square$

An straightforward consequence of 1.2 and 1.3 is theorem A:

Theorem 1.5. *A topos $\mathcal{E}$ with a representable point $\mathcal{E}ns \xrightarrow{p} \mathcal{E}$, $p^* = [A, -]$, $A \in \mathcal{E}$ is connected atomic if and only if it is the classifying topos $\mathcal{B}G$ of a discrete group G, and this group can be taken to be $Aut(A)^{op}$.*

Proof. By theorem 1.2 the functor $[A, -]$ lifts into the category of transitive G-sets, for $G = [A, A]^{op} = Aut(A)^{op}$ (1.4). Theorem 1.3 then essentially means that this lifting is full and faithful. Since every transitive G-set is a quotient of the G-set $[A, X]$ *for* $X = A$, it follows (by the comparison lemma ([1], Expose III, 4.) that the topos of sheaves for the canonical topology on $\mathcal{C}$ is equivalent to the topos of G-sets.

It is immediate to check (see 8.1) that the data in assumption 1.1 is a connected atomic site with a representable point, and any connected atomic topos with a representable point can be presented in this way (see [2]). This finishes the proof. $\square$

2. THE THEOREMS OF LOCALIC GALOIS THEORY

This corresponds to the prorepresentable case of the theory.

Let $\mathcal{C}$ be any category and $P \in Pro\,\mathcal{C}$ be any pro-object (in the sense of Grothendieck [1]). Recall that the proobject P is the formal dual of a prorepresentable functor $F : \mathcal{C} \longrightarrow \mathcal{E}ns$, $F = [P, -]$. We shall call the functor F to be the *fiber functor*.

Assume:

Assumption 2.1.
  i) Every arrow $Y \longrightarrow X$ in $\mathcal{C}$ is an strict epimorphism.
  ii) For every $X \in \mathcal{C}$ there exists $P \longrightarrow X$. That is, $FX \neq \emptyset$.
  iii) The prorepresentable functor $F = [P, -]$ preserves strict epimorphisms.

Then:

Theorem 2.2. *For every object $X \in \mathcal{C}$ the action of the localic group of automorphisms $lAut(P)^{op} = lAut(F)$ on the set $[P, X] = FX$ is transitive.*

Theorem 2.3. *Every arrow $P \xrightarrow{x} X$ in $\mathcal{C}$ is the categorical quotient, relative to the category $\mathcal{C}$, of P by the action of the Galois group $lFix(x) \in lAut(P)$ described informally as $\{h \in Aut(P) \,|\, xh = x\}$.*

The equivalent version of this statement in terms of the fiber functor is reminiscent of the lifting lemma in classical covering theory:

Lifting Lemma: Given any objects $X \in \mathcal{C}$, $Y \in \mathcal{C}$, and elements $x \in FX$, $y \in FY$, if $lFix(x) \leq lFix(y)$ in $lAut(F)$, then there exist a unique arrow $X \xrightarrow{f} Y$ in $\mathcal{C}$ such that $F(f)(x) = y$.

In the rest of this paper we shall explain and prove these theorems, giving the necessary definitions.

3. Preliminaries on Localic Spaces and Groups

Topoi are often considered as generalized topological spaces, but the intuition in topos theory is not only geometrical. We think of locale theory as a reflection of topos theory (with the poset $2 = \{0, 1\}$ playing the role of the category $\mathcal{E}ns$ of sets), as well as that of a theory of generalized topological spaces.

We consider a *poset* as a category, and in this vein a *partial order* is a reflexive and transitive relation, not necesarially antisymetric. We denote the order relation either by $" \rightarrow "$ or by $" \leq "$. We shall call *objects* the elements of a poset.

A morphism of posets is an *injection* when it is injective in the isomorphism classes. That is, if it creates isomorphisms.

A *locale* is a complete lattice in which finite infima distribute over arbitrary suprema. A morphism of locales $E \xrightarrow{f^*} H$ is defined to be a function f^* preserving finite infima and arbitrary suprema (notice that we put automatically an upper star to indicate that these arrows are to be considered as inverse images of geometric maps). We shall also refer to such a morphism as *an H-valued point of E*. 2-valued points $E \xrightarrow{f^*} 2$ are just called *points*.

Inf-lattices D are sites of definition for locales (rather than bases of opens). 2-valued *presheaves* $D^{op} \rightarrow 2$ correspond to downward closed subsets T, and they form a locale, $D^{\wedge} = 2^{D^{op}}$. Given a Grothendieck (pre) topology on D, 2-valued *sheaves* are those T such that for each cover $u_\alpha \rightarrow u$, $(\forall \alpha \ u_\alpha \in T) \quad \Rightarrow \quad (u \in T)$, and they also form a locale, denoted $D^{\sim}$. The associated sheaf defines a morphism of locales $D^{\wedge} \rightarrow D^{\sim}$, and this is a procedure in which quotients of locales are obtained. A *site* is in this sense a *presentation* of the locale of sheaves.

An *H-valued point* of an inf-lattice is an inf-preserving morphism into a locale H. When $H = 2$, it corresponds to an upward closed subset P such that $u \in P$, $w \in P \Rightarrow u \wedge w \in P$. An H-valued point of a site in addition must send covers into epimorphic families. When

$H = 2$, this corresponds to the usual requirement. That is, for each cover $u_\alpha \to u$, $(u \in P) \Rightarrow (\exists \alpha \ u_\alpha \in P)$.

The basic result of this construction is that the associate sheaf $D \xrightarrow{\#} D^\sim$ is a point which is generic, in the sense that giving any locale H, composing with $\#$ defines an equivalence of posets $\mathcal{P}oints(D^\sim, H) \xrightarrow{\simeq} \mathcal{P}oints(D, H)$. *Points of a site of definition and of the locale of sheaves are the same thing.*

A *localic space* is the formal dual of a local. Thus, $E \xrightarrow{f^*} H$ defines a map or morphism of localic spaces from H to E, $H \xrightarrow{f} E$. Following [4], all these maps are called *continuous maps*. A *point* of a localic space E is a point of the corresponding locale.

A function preserving finite infima is an injection if and only if it reflects isomorphisms (recall that finite infima determines the order relation).

A *surjection* between localic spaces is a map whose inverse image reflects isomorphisms. A locale has *enough points* if its family of points is (collectively) surjective.

Any local E determines a topology (in the classical sense) on its set of points by means of the correspondence, for $u \in E$, $P \in \mathcal{P}oints(E)$ and $U \subset \mathcal{P}oints(E)$: $P \in U \Leftrightarrow u \in P$.

A localic space is a (sober) topological space if and only if it has enough points. In this case, the topology in $\mathcal{P}oints(E)$ also determines E since $u \simeq v \Leftrightarrow U = V$.

A *localic monoid*, (resp. *localic group*) is a monoid object (resp. group object) in the category of localic spaces. A *morphism of monoids (or groups)* $H \xrightarrow{\varphi} G$ is a continuous map such that $m^* \varphi^* = (\varphi^* \otimes \varphi^*) m^*$ (where m denotes the multiplication in the two structures).

We recall now a construction of the free inf-lattice on a poset D. That is, the inf-completion of D, which is the inf-lattice $\mathcal{D}(D)$ whose points $\mathcal{D}(D) \to H$ correspond exactly to the order preserving morphisms $D \to H$. Warning: these are not the points of D !.

Proposition 3.1. *Given any poset D, consider the diagram:*

$$D \overset{Yoneda}{\underset{\hookrightarrow}{\quad\longrightarrow\quad}} \mathcal{D}(D) \hookrightarrow (2^D)^{op}$$

where $\mathcal{D}(D) \subset (2^D)^{op}$ is the full subposet of finitely generated upward closed subsets of D. Given a finite subset $\{a_1, \dots, a_n\} \subset D$, We denote $[A] = [<a_1>, \dots, <a_n>] = \{a \in D \mid \exists i \ a_i \le a\}$. If $[B] = [<b_1>, \dots, <b_k>]$, then $[A] \to [B]$ in $\mathcal{D}(D)$ (that is $[B] \subset [A]$) if and only if $\exists \sigma : \{1, \dots, k\} \longrightarrow \{1, \dots, n\}$, $a_{\sigma i} \le b_i$.

A particular case of this construction is the free inf-lattice on a set X, $\mathcal{D}(X)$, which is the poset of finite subsets of X with the reverse of the natural order. It follows that the free locale on X is the locale of presheaves on $\mathcal{D}(X)$, $\mathcal{L}(X) = \mathcal{D}(X)^{\wedge}$.

The points of $\mathcal{L}(X)$ are (by definition) the subsets of X. If $x \in X$, we denote $[<x>]$ the corresponding generator in $\mathcal{L}(X)$. If $S \subset X$, we have $S \in [<x>] \Leftrightarrow x \in S$. Similarly, if $\{x_1, \dots, x_n\} \subset X$, we write $[< x_1 >, \dots, < x_n >]$ for the corresponding object in $\mathcal{D}(X) \subset \mathcal{L}(X)$. Notice that this object defines the open set (in the topological space of points) $\{S \subset X \mid x_i \in S,\ i = 1, \dots, n\}$. The following is clear:

Proposition 3.2. *The locale of relations $lRel(X)$ on a set X is the free locale $\mathcal{L}(X \times X) = \mathcal{D}(X \times X)^{\wedge}$. If $\{(x_1,\, y_1) \dots, (x_n,\, y_n)\} \subset X \times X$, we write $[< x_1 \mid y_1 > \dots, < x_n \mid y_n >]$ for the corresponding object in the site or in the locale.*

We take now from [5] a site of definition for the localic group of automorphisms of a set. That is, a localic group such that its points are the automorphisms of X.

Proposition 3.3. *The locale of automorphisms $lAut(X)$ on a set X is the locale of sheaves on the site with underline poset the inf-lattice $\mathcal{D}(X \times X)$, and with the covers generated by the following families (in the notation in 3.2)::*

$$\emptyset \;\to\; [<z \mid x>,\ <z \mid y>]\,,$$
$$\emptyset \;\to\; [<x \mid z>,\ <y \mid z>]\,,$$
$$(each\ x,\ y,\ z,\ x \neq y)$$
$$[<x \mid z>] \;\to\; 1,\ x \in X\,,$$
$$[<z \mid x>] \;\to\; 1,\ x \in X\,,$$
$$(each\ z)\,.$$

Proof. It follows immediately from 3.2. The coverings above force a relation to be, in turn, univalued, injective, everywhere defined, and surjective. □

We shall abuse the notation and omit to indicate the associate sheaf morphism $lRel(X) \to lAut(X)$. Thus, $[< x_1 \mid y_1 > \dots, < x_n \mid y_n >]$ also denotes the corresponding object in $lAut(x)$.

Actually, this locale has enough points, and it is the usual set of bijections of X furnished with the product topology. We have then the usual open set in the base of this topology $\{f: X \to X \mid f(x_i) = y_i\ i = 1, \dots, n\}$.

The motivation in G. Wraith paper was to consider this presentation in an arbitrary topos, where it defines a local which in general will not have enough points.

The local $lRel(X)$ is a localic monoid, and its binary operation restricts to $lAut(X)$ and defines a localic group. This structure is given

by:

$$m^*([<x\,|\,y>]) \;=\; \bigvee_z \,[<x\,|\,z>] \otimes [<z\,|\,y>]$$

The identity map $X \to X$ determines a point $lAut(X) \xrightarrow{e^*} 2$ which is the neutral element for m: $e^*[<x\,|\,y>] \;=\; 1 \;\;\Leftrightarrow\;\; x \;=\; y$. Thus $e \in [<x\,|\,y>] \;\Leftrightarrow\; x \;=\; y$.

All this is described in [5], from were we take also the definition of *action* of a localic group G on a set X, see 7.1 below.

4. The locale of automorphisms of a set-valued functor

Recall that given any category $\mathcal{C}$ and any functor $\mathcal{C} \xrightarrow{F} \mathcal{E}ns$, the diagram of F, that we denote Γ_F, is the category whose objects are the elements of the disjoint union of the sets FX, $X \in \mathcal{C}$. That is, pairs (x, X) where $x \in FX$. The arrows $(x, X) \xrightarrow{f} (y, Y)$ are maps $X \xrightarrow{f} Y$ such that $F(f)(x) = y$. There is a diagram

$$\Gamma_F{}^{op} \longrightarrow \mathcal{E}ns^{\mathcal{C}}$$
$$(x, X) \longmapsto [X, -]$$

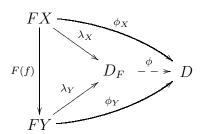with the obvious definition on arrows, and F is the colimit of this diagram.

Definition 4.1. We define a poset, that we denote D_F, by the following rule:

$$\frac{(x,\ X) \le (y,\ Y)}{\exists\ X \xrightarrow{f} Y\ F(f)(x) = y}$$

Consider the function $FX \xrightarrow{\lambda_X} D_F$ defined by $\lambda_X(x) = (X,\ x)$. The proof of the following proposition is immediate:

Proposition 4.2. *The poset D_F has, and therefore it is characterized, by the following universal property:*

For each $X \in \mathcal{C}$, there is a function $FX \xrightarrow{\lambda_X} D_F$, and for each $X \xrightarrow{f} Y$ a transformation $\lambda_X \to \lambda_Y \circ F(f)$ (that is, for each $x \in FX$, $\lambda_X(x) \;\le\; (\lambda_Y \circ F(f))(x)$). And for any other such data, there is a unique morphisms of posets ϕ (as indicated in the diagram below) such that $\phi \circ \lambda_X \;=\; \phi_X$, $\phi \circ \lambda_Y \;=\; \phi_Y$:

Definition 4.3. A *natural relation* is a relation $R \subset F \times F$ in the functor category. That is, it is a family of relations RX on FX, $X \in \mathcal{C}$, such that given any arrow $X \xrightarrow{f} Y$ in $\mathcal{C}$, and $(x_0, x_1) \in FX \times FX$:

$$(x_0, x_1) \in RX \quad \Rightarrow \quad (F(f)(x_0),\ F(f)(x_1)) \in RY$$

In other terms, it is a family of functions $FX \times FX \xrightarrow{\phi_X} 2$ such that

$$\phi_X(x_0, x_1) \ \le \ (\phi_Y \circ (F(f) \times F(f)))(x_0, x_1)$$

It is clear that if a natural relation is functional, then it is a natural transformation.

Consider the composite of the diagonal functor $\mathcal{C} \to \mathcal{C} \times \mathcal{C}$ with $F \times F$, that we denote ΔF, $(\Delta F)(X) = FX \times FX$. Notice that there is a full and faithful inclusion of categories $\Gamma_F \hookrightarrow \Gamma_{\Delta F}$ and consequently a full inclusion of posets $D_F \hookrightarrow D_{\Delta F}$.
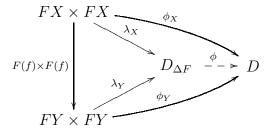
From proposition 4.2 it follows immediately (see also definition 4.1):

Proposition 4.4 (Generic Natural Relation). *The poset $D_{\Delta F}$ has, and therefore it is characterized, by the following universal property:*

For each $X \in \mathcal{C}$, there is a function $FX \times FX \xrightarrow{\lambda_X} D_{\Delta F}$, and for each $X \xrightarrow{f} Y$ a transformation $\lambda_X \to \lambda_Y \circ (F(f) \times F(f))$. That is, for each $(x_0, x_1) \in FX \times FX$,

$$\lambda_X(x_0, x_1) \ \le \ (\lambda_Y \circ (F(f) \times F(f)))(x_0, x_1)$$

And for any other such data, there is a unique morphisms of posets ϕ (as indicated in the diagram below) such that $\phi \circ \lambda_X = \phi_X$, $\phi \circ \lambda_Y = \phi_Y$:

It follows that a morphisms of posets $D_{\Delta F} \to 2$ corresponds exactly to the data defining a natural relation of F.

Corollary 4.5. *The points of the locale of presheaves $\mathcal{D}(D_{\Delta F})^{\wedge}$ on the free inf-lattice $\mathcal{D}(D_{\Delta F})$ on the poset $D_{\Delta F}$ are exactly the natural relations of F. That is, $lRel(F) = \mathcal{D}(D_{\Delta F})^{\wedge}$*

For later reference, and according with 3.2 and 3.1, we record:

Notation 4.6. By definition, the set of objects of $D_{\Delta F}$ is the disjoint union of the sets $FX \times FX$, $X \in \mathcal{C}$. Given an element $(X, (x_0, x_1))$ and a finite subset $A \subset D_{\Delta F}$ of this set, we denote

$$[(X, <x_0 \,|\, x_1>),\ A] \ = \ [\{(X, (x_0, x_1))\} \cup A] \ = \ [(X, <x_0 \,|\, x_1>)] \wedge [A]$$

the corresponding object in $\mathcal{D}(D_{\Delta F})$.

We shall construct now the locale of automorphisms of a set valued functor F by defining a site structure on the inf-lattice $\mathcal{D}(D_{\Delta F})$.

Proposition 4.7. *The locale of automorphisms $lAut(F)$ of a set-valued functor F is the locale of sheaves on the site with underline poset the inf-lattice $\mathcal{D}(D_{\Delta F})$, and with the covers generated by the following families:*

$$\emptyset \rightarrow [(X, <z\,|\,x>), (X, <z\,|\,y>)]\,,$$
$$\emptyset \rightarrow [(X, <x\,|\,z>), (X, <y\,|\,z>)]\,,$$
$$\text{(each } X, \text{ and each } x \neq y, \ z \in FX)$$
$$[(X, <x\,|\,z>)] \rightarrow 1, \ x \in FX\,,$$
$$[(X, <z\,|\,x>)] \rightarrow 1, \ x \in FX\,,$$
$$\text{(each } X \text{ and each } z \in FX)\,.$$

Recall that the object $[(X_1, <x_1\,|\,y_1>) \ldots , (X_n, <x_n\,|\,y_n>)]$ corresponds to the open set $\{\phi : F \rightarrow F \mid \phi X_i(x_i) = y_i\}$

Proof. It follows immediately from 3.3 and 4.5. $\square$

For each $X \in \mathcal{C}$ the map $FX \times FX \xrightarrow{\lambda_X} \mathcal{D}(D_{\Delta F})$, defined by $\lambda_X^*[< x_0\,|\,x_1 >] = [(X, < x_0\,|\,x_1 >)]$ determines a morphism of locales $lRel(F) \xrightarrow{\lambda_X} lRel(FX)$.

The locale $lRel(F)$ is a localic monoid with the binary operation m defined by $m^*[(X, <x\,|\,y>] = \lambda_X^* m_X^*[<x\,|\,y>]$, and by definition the arrow λ_X becomes a morphism of monoids. This operation on $lRel(F)$ restricts and defines the group structure of $lAut(F)$.

Consider now the morphism of locales given by the associate sheaf $\mathcal{D}(D_{\Delta F}) \hookrightarrow lRel(F) \xrightarrow{\#} lAut(F)$. We have:

Proposition 4.8. *For each object $X \in \mathcal{C}$, the composite of the maps:*

$$FX \times FX \xrightarrow{\lambda_X} \mathcal{D}(D_{\Delta F}) \xrightarrow{\#} lAut(F)$$

$(\#\,\lambda_X)([< x_0\,|\,x_1 >]) = \#[(X, < x_0\,|\,x_1 >)]$, determines a morphism of locales $lAut(FX) \rightarrow lAut(F)$ that defines an action of $lAut(F)$ on the set FX. Furthermore, given any arrow $X \xrightarrow{f} Y$, the function $FX \xrightarrow{F(f)} FY$ becomes a morphism of actions (see section 6).

Proof. For the first assertion it suffices to show that this map sends covers into covers on the respective sites of definition. But this is clear. The second assertion follows by the diagram in 4.4. $\square$

Remark 4.9. *The identity $F \rightarrow F$ determines a point $lAut(F) \xrightarrow{e^*} 2$ given by $e^*[(X, <x\,|\,z>)] = 1 \Leftrightarrow x = z$. This point is the neutral element for the group structure. We have $e \in [(X, <x\,|\,z>)] \Leftrightarrow x = z$.*

5. The (pre)topology generated by a family of covers

Suppose we have a category $\mathcal{D}$ (with finite limits to simplify), and a family of *(basic) covers* $D_\alpha \to D$ on some objects $D \in \mathcal{D}$. We consider the site determined by the (pre)-topology generated by these covers. To check that a finite limit preserving functor is a point for this site it is enough to test the point condition only on the basic covers. To check that a presheaf is a sheaf, it is enough to test the sheaf condition on all covers obtained by pulling-back basic covers (in some terminology, the *covering system* generated by the basic covers). However, in this paper we have to deal with a more subtle problem. We have to check that a given presheaf T (which is not a sheaf) behaves as a sheaf against some given objects $A \in \mathcal{D}$. In this case, it is necessary to test the sheaf condition on all the covers $A_\alpha \to A$ of the (pre)-topology generated. This is so because T may not be a sheaf against the objects A_α, and this fact breaks the argument used to show that it is enough to test the sheaf condition on the covering system.

We need a careful description (by transfinite induction) of the (pre) topology generated by a family of basic covers.

First we shall fix some notation. Let Cov be a collection of *small* families $A_\alpha \to A \in Cov(A)$ of arrows (to be considered as *coverings*) on each object $A \in \mathcal{D}$ (small in the sense that the index α ranges over a set in $\mathcal{E}ns$). Given a collection Cov, define a new collection, denoted πCov:

$$A_\alpha \to A \;\in\; \pi Cov(A) \;\iff\; \exists\, B_\alpha \to B \;\in\; Cov(B)$$

$$and\ a\ pullback \quad
\begin{array}{ccc}
A_\alpha & \longrightarrow & A \\
\downarrow & & \downarrow \\
B_\alpha & \longrightarrow & B
\end{array}$$

Given another collection Dov, define the *composite* $Dov \circ Cov$ by means of the following implication:

$$A_\alpha \to A \;\in\; Cov(A) \;\; and \;\; \forall \alpha \;\; A_{\alpha,\beta} \to A_\alpha \;\in\; Dov(A_\alpha)$$
$$\implies \;\; A_{\alpha,\beta} \to A_\alpha \to A \;\in\; (Dov \circ Cov)(A)$$

Notice that collections compose the other way than arrows, and that the two constructions above preserve the size condition. Let Iso be the collection whose covers consists of a single isomorphism.

A *covering system* is a collection Cov such that $Iso \subset Cov$ and $\pi Cov \subset Cov$. A covering system is a *(pre) topology* if in addition $Cov \circ Cov \subset Cov$.

Proposition 5.1. *Let $\mathcal{D}$ be a category with finite limits, and $D_\alpha \to D \in Dov(D)$ be a collection of families of arrows (to be considered as basic covers on some basic objects D).*

Define $Cov_0 = Iso \cup Dov$, *and:*
$Cov_1 = \pi Cov_0$.
for an ordinal $\rho + 1$, $Cov_{\rho+1} = Cov_\rho \circ Cov_1$.
for a limit ordinal ρ, $Cov_\rho = \bigcup_{\nu < \rho} Cov_\nu$.

Then
1) $\forall \nu < \rho$ $Cov_\nu \subset Cov_\rho$.
2) $\forall \rho$ Cov_ρ *is a covering system.*
3) $\forall \rho, \nu$ $Cov_\rho \circ Cov_\nu \subset Cov_{\rho+\nu}$ *(actually, equality holds).*

Proof. 1) is clear, 2) follows easily by induction. 3) follows for each ρ by induction on ν; on $\nu + 1$ by associativity, and on limit ordinals it is straightforward. $\square$

Proposition 5.2. *With the notation in the previous proposition,* $Cov = \bigcup_{all\ \rho} Cov_\rho$ *is the (pre) topology generated by* Dov.

Proof. It is clearly a covering system by 5.1,2). It remains to see it is closed under composition. Consider $A_{\alpha,\beta} \to A_\alpha \to A$, with $A_\alpha \to A \in Cov_\nu(A)$, and $A_{\alpha,\beta} \to A_\alpha \in Cov_{\rho_\alpha}(A_\alpha)$. Take an ordinal ρ such that $\rho \geq \rho_\alpha$ $\forall \alpha$ and use 5.1,1) and 5.1,3). $\square$

6. PROOF OF THE THEOREMS 2.2 AND 2.3

IN THIS SECTION WE ASSUME THE VALIDITY OF 2.1

In [1], Expose I, 10.2 and 10.3 Grothendieck defines the important concept of *strict epimorphism*. Since then a whole variety of equivalent and/or related versions of this notion appeared in the literature under all sorts of names. To avoid confusion and fix the notation we recall now this original definition.

Let $X \xrightarrow{f} Y$ be an arrow in a category $\mathcal{C}$ and let Ker_f be the full subcategory of the appropriate slice category whose objects are pairs of arrows $C \begin{smallmatrix} x \\ \longrightarrow \\ \longrightarrow \\ y \end{smallmatrix} X$ such that $fx = fy$. Then:

Definition 6.1. f is an *strict epimorphism* if for any other arrow $X \xrightarrow{g} Z$ such that $Ker_f \subset Ker_g$, there exists a unique $Y \xrightarrow{h} Z$ such that $g = hf$. When Ker_f has a terminal object the strict epimorphism is called *effective*.

It immediately follows that strict epimorphisms are epimorphisms and that *strict epi + mono = iso.*

Proposition 6.2. *The diagram of* F, Γ_F, *is a cofiltered category, and it is already a poset,* $\Gamma_F = D_F$.

Proof. By definition of prorepresentable functor, Γ_F is a cofiltered category. Since all maps $X \xrightarrow{f} Y$ in $\mathcal{C}$ are epimorphisms, for any

object $Z \in \mathcal{C}$ the transition morphisms corresponding to an arrow $(x, X) \xrightarrow{f} (y, Y)$ in Γ_F, $f^* : [Y, Z] \longrightarrow [X, Z]$ are all injective functions. By construction of filtered colimits in $\mathcal{E}ns$ it follows that the canonical maps of the colimit $[X, -] \xrightarrow{x} F$ are injective natural transformations (thus monomorphisms in the category $\mathcal{E}ns^{\mathcal{C}}$). This implies that Γ_F is a poset.   □

Proposition 6.3. *The functor F is faithful and reflects isomorphisms.*

Proof. Let $X \xrightarrow{f} Y$ be such that $F(f)$ is an isomorphism. We shall see that f is a monomorphism (and thus, by 2.1 i), an isomorphism). Let $Z \mathrel{\substack{t \\ \longrightarrow \\ \longrightarrow \\ s}} X$ be such that $fs = ft$. Clearly it follows that $F(s) = F(t)$. Take any $z \in FZ$ (use 2.1 ii) and let $x = F(s)(z) = F(t)(z)$. In this way s and t define arrows $(Z, z) \longrightarrow (X, x)$ in Γ_F. It follows from 6.2 that we must have $s = t$. Observe that within this argument we have also shown that F is faithful.   □

Recall now the construction 4.7 of the locale $lAut(F)$.

Definition 6.4. Given an object $[A]$ (determined by a finite subset $A \subset D_{\Delta F}$) on the site of definition $\mathcal{D}(D_{\Delta F})$, the *content* of $[A]$ is the set of generators which are below $[A]$. That is, it is the set of objects $[(M, < m_0 | m_1 >)]$, $M \in \mathcal{C}$, $(m_0, m_1) \in FM \times FM$ such that $[(M, < m_0 | m_1 >)] \leq [A]$. Notice that this means $[(M, <m_0 | m_1 >)] \leq [(X, <x_0 | x_1 >)]$ for each $(X, (x_0, x_1)) \in A$, which in turn means that there is an arrow $M \xrightarrow{f} X$ in $\mathcal{C}$ such that $f(m_0) = x_0$, $f(m_1) = x_1$ (see 3.1 and 4.1).

Proposition 6.5. *For each $X \in \mathcal{C}$, and each $x \neq y, z \in FX$, $[(X, <x | z>), (X, <y | z>)]$ and $[(X, <z | x>), (X, <z | y>)]$ in $\mathcal{D}(D_{\Delta F})$ have empty content.*

Proof. Let $[(M, < m_0 | m_1 >)] \leq [(X, < x | z >), (X, < y | z >)]$. Then, there are arrows $M \xrightarrow{f} X$ and $M \xrightarrow{g} X$ such that $f(m_0) = x$, $f(m_1) = z$, $g(m_0) = y$, $g(m_1) = z$. It follows from 6.2 that $f = g$, thus $x = y$, contrary with the assumption. In the second case we do in the same way.   □

Proposition 6.6. *Let $W \xrightarrow{f} X$ and $W \xrightarrow{g} Y$ be any two arrows in $\mathcal{C}$, and $x_0 \in FX$, $y_0 \in FY$. If for $w \in FW$ the implication $F(f)(w) = x_0 \Rightarrow F(g)(w) = y_0$ holds, then there exists a unique $X \xrightarrow{h} Y$ such that $g = hf$ and $F(h)(x_0) = y_0$.*

Proof. We prove first that under the assumption in the proposition, for arbitrary $v \in FW$, $w \in FW$, the following implication holds:

$$1) \quad F(f)(v) = F(f)(w) \Rightarrow F(g)(v) = F(g)(w)$$

Take M, $m \in FM$ and $M \xrightarrow{s} W$, $M \xrightarrow{t} W$ such that $F(s)(m) = v$, $F(t)(m) = w$ (recall Γ_F is cofiltered). It follows that $F(fs)(m) = F(ft)(m)$, thus by 6.2 $fs = ft$. By 2.1 i), iii) take $m_0 \in FM$ such that $F(fs)(m_0) = F(ft)(m_0) = x_0$. Let $v_0 = F(s)(m_0)$, $w_0 = F(t)(m_0)$. Clearly,

$$[(M, <m, m_0>)] \to [(W, <v, v_0>), (W, <w, w_0>)]$$

and $F(f)(v_0) = F(f)(w_0) = x_0$. We have also

$$[(W, <v, v_0>)] \to [(Y, <F(g)(v), F(g)(v_0)>)]$$

$$[(W, <w, w_0>)] \to [(Y, <F(g)(w), F(g)(w_0)>)]$$

By assumption $F(g)(v_0) = F(g)(w_0) = y_0$. Thus, we have

$$[(M, <m, m_0>)] \to [(Y, <F(g)(v), y_0)>), (Y, <F(g)(w), y_0)>)]$$

It follows then from 6.5 that we must have $F(g)(v) = F(g)(w)$. This finishes the proof of 1).

It follows from 1) that $Ker_{F(f)} \subset Ker_{F(g)}$. Since F is faithful (6.3) this implies $Ker_f \subset Ker_g$. The proof finishes by definition of strict epimorphism (6.1). $\qquad\square$

Our first important result is the following:

Theorem 6.7. *Let* $[A_\alpha] \to [A]$ *in* $\mathcal{D}(D_{\Delta F})$ *be any cover in the site of definition of* $lAut(F)$ *(see 4.7). Then, if* $[A]$ *has nonempty content, there exists an index* α *such that* $[A_\alpha]$ *has non empty content.*

Proof. By induction on the generation of covers (see 5.1 and 5.2).

1) Let [D] be the object in the two basic empty covers:
$[D] = [(X, <x\,|\,z>), (X, <y\,|\,z>)]$ or $[(X, <z\,|\,x>), (X, <z\,|\,y>)]$,
By 6.5 a pullback of the form

$$\begin{array}{ccc} \emptyset & \longrightarrow & [A] \\ \downarrow & & \downarrow \\ \emptyset & \longrightarrow & [D] \end{array}$$

can not be, since it implies that $[D]$ would have non empty content.

Consider now $[D] = 1$, $Z \in \mathcal{C}$, $z_1 \in FZ$, the basic cover $[(Z, <z\,|\,z_1>)] \to 1$, $z \in FZ$, and the pullback (see 4.6):

$$\begin{array}{ccc} [(Z, <z\,|\,z_1>), A] & \longrightarrow & [A] \\ \downarrow & & \downarrow \\ [(Z, <z\,|\,z_1>)] & \longrightarrow & 1 \end{array}$$

Let $[(M, <m_0\,|\,m_1>)] \leq [A]$, and take $(N, n_1) \to (Z, z_1)$, $(N, n_1) \to (M, m_1)$ in Γ_F. Since the function $FN \to FM$ is surjective (2.1), we can take $n_0 \in FN$ such that $n_0 \mapsto m_0$,

and let z_0 be the image of n_0 in FZ, $n_0 \mapsto z_0$. We have then $[(N, <n_0 \,|\, n_1>)] \leq [(Z, <z_0 \,|\, z_1>)\,, (M, <m_0 \,|\, m_1>)]$. This shows that $[(Z, <z_0 \,|\, z_1>), A]$ (corresponding to the index z_0 in the cover) has non empty content.

The same argument applies to the remaining basic covers $[(Z, <z_0 \,|\, z>)] \to 1$, $z \in FZ$.

$\rho + 1)$ Consider now the cover $[A_{\alpha, \beta}] \to [A_\alpha] \to [A]$, with $[A_{\alpha, \beta}] \to [A_\alpha] \in Cov_\rho$ and $[A_\alpha] \to [A] \in Cov_1$. Take α such that $[A_\alpha]$ has non empty content, and for this α take β such that $[A_{\alpha, \beta}]$ has non empty content.

limit ordinal ρ) In this case the proof is even more immediate. $\quad\square$

Corollary 6.8. *If $[A] \in \mathcal{D}(D_{\Delta F})$ has non empty content, then the empty family does not cover $[A]$. In particular, for any $X \in \mathcal{C}$, $(x_0, x_1) \in FX \times FX$, the empty family does not cover $[(X, <x_0 \,|\, x_1>)]$.*

Proof. Clear, since for the empty cover can not exist any index. $\quad\square$

The fact that the empty family does not cover $[(X, <x_0 \,|\, x_1>)]$ means that this object stays different from 0 in the sheaf poset.

This proves theorem 2.2.

Corollary 6.9 (Theorem 2.2). *For each $X \in \mathcal{C}$, the action of $lAut(F)$ on the set FX (defined in 4.8) is transitive. Explicitly, $\forall\, (x_0, x_1) \in FX \times FX$, $\#[(X, <x_0 \,|\, x_1>)] \neq 0$ (see 7.1).*

Our second important result is the following:

Theorem 6.10. *Given two objects $[(X, <x_0 \,|\, x_1>)]$, $[(Y, <y_0 \,|\, y_1>)]$ in $D_{\Delta F}$, and a cover$[A_\alpha] \to [(X, <x_0 \,|\, x_1>)]$ in $\mathcal{D}(D_{\Delta F})$ in the site of definition of $lAut(F)$ (see 4.7), the following implication holds:*

$$\forall\, \alpha\, [A_\alpha] \to [(Y, <y_0 \,|\, y_1>)] \implies [(X, <x_0 \,|\, x_1>)] \to [(Y, <y_0 \,|\, y_1>)]$$

Proof. Consider first that by the corollary above a cover of $[(X, <x_0 \,|\, x_1>)]$ can not be empty. Let now $[(Z, <z \,|\, z_1>)] \to 1$, $z \in FZ$ be one of the other basic covers, and consider the Cov_1 cover determined by following pull-back:

$$
\begin{array}{ccc}
[(Z, <z \,|\, z_1>), (X, <x_0 \,|\, x_1>)] & \longrightarrow & [(X, <x_0 \,|\, x_1>)] \\
\downarrow & & \downarrow \\
[(Z, <z \,|\, z_1>)] & \longrightarrow & 1
\end{array}
$$

Take $(M, m_1) \to (Z, z_1)$, $(M, m_1) \to (X, x_1)$ in Γ_F. Consider all the $m \in FM$ such that $m \mapsto x_0$, and let z be the images of these m in FZ, $m \mapsto z$. This defines, for each such m

$$[(M, <m \,|\, m_1>)] \to [(Z, <z \,|\, z_1>), (X, <x_0 \,|\, x_1>)].$$

We start now the induction on the generation of covers (see 5.1 and 5.2). We deal simultaneously with the case $\rho = 1$ and the case $\rho + 1$. Consider the $Cov_{\rho+1}$ cover determined by a Cov_1 cover as above, and for each $z \in FZ$, a Cov_ρ cover

$$[A_{z,\,\alpha}] \rightarrow [(Z, <z \,|\, z_1>),\ (X, <x_0 \,|\, x_1>)]$$

(the case $\rho = 1$ is included considering all these covers to be the identity).

For each m (and z, $m \mapsto z$) as above, consider the following diagram, defined as a pullback in $\mathcal{D}(D_{\Delta F})$

$$
\begin{array}{ccc}
[B_{z,\,\alpha}] & \longrightarrow & [(M, <m \,|\, m_1>)] \\
\downarrow & & \downarrow \\
[A_{z,\,\alpha}] & \longrightarrow & [(Z, <z \,|\, z_1>),\ (X, <x_0 \,|\, x_1>)]
\end{array}
$$

By assumption, for each α, there is $[A_{z,\,\alpha}] \rightarrow [(Y, <y_0 \,|\, y_1>)]$. Composing we have $[B_{z,\,\alpha}] \rightarrow [(Y, <y_0 \,|\, y_1>)]$. Finally, by 5.1, 2) and the inductive hypothesis we have $[(M, <m \,|\, m_1>)] \rightarrow [(Y, <y_0 \,|\, y_1>)]$. Since all these arrows (one for each m) send $m_1 \mapsto y_1$, by 6.2 they all correspond to a same single arrow $M \rightarrow Y$ in $\mathcal{C}$.

In conclusion, we have two arrows $M \rightarrow X$, $M \rightarrow Y$ such that for $m \in FM$, if $m \mapsto x_0$, then $m \mapsto y_0$. It follows by 6.6 that there exist $X \rightarrow Y$ such that $x_0 \mapsto y_0$. Since the composite $M \rightarrow X \rightarrow Y$ is the arrow $M \rightarrow Y$, it is also the case that $x_1 \mapsto y_1$. Thus we have $[(X, <x_0 \,|\, x_1>)] \rightarrow [(Y, <y_0 \,|\, y_1>)]$.

The same argument applies to the other remaining basic covers $[(Z, <z_0 \,|\, z>)] \rightarrow 1$, $z \in FZ$.

The case of a limit ordinal is evident. This finishes the proof $\qquad\square$

Clearly the topology on $\mathcal{D}(D_{\Delta F})$ that defines $lAut(F)$ is not subcanonical, and so the morphism of inf-posets $\mathcal{D}(D_{\Delta F}) \xrightarrow{\#} lAut(F)$ (where $\#$ indicates the associated sheaf) is far from being full. However, for the full subposet $D_{\Delta F} \hookrightarrow \mathcal{D}(D_{\Delta F})$ the theorem above gives:

Corollary 6.11. *The morphism of posets $D_{\Delta F} \xrightarrow{\#} lAut(F)$ is full. Explicitly, if $\#[(X, <x_0 \,|\, x_1>)] \rightarrow \#[(Y, <y_0 \,|\, y_1>)]$ in $lAut(F)$, then there exists a unique $X \rightarrow Y$ in $\mathcal{C}$ such that $x_0 \mapsto y_0$ and $x_1 \mapsto y_1$.*

Proof. Consider the following chain of equivalences (or bijections) justified, in turn, by definition of $\#$, (Yoneda and) construction of $\#$, and theorem 6.10 respectively:

$$\frac{\#[(X,\ <x_0\,|\,x_1>)] \rightarrow \#[(Y,\ <y_0\,|\,y_1>)]}{[(X,\ <x_0\,|\,x_1>)] \rightarrow \#[(Y,\ <y_0\,|\,y_1>)]}$$

$$\frac{\exists\ cover\ [A_\alpha] \rightarrow [(X,\ <x_0\,|\,x_1>)]\ |\ \ \forall\,\alpha\ [A_\alpha] \rightarrow [(Y,\ <y_0\,|\,y_1>)]}{[(X,\ <x_0\,|\,x_1>)] \rightarrow [(Y,\ <y_0\,|\,y_1>)]}$$

$\square$

This proves theorem 2.3.

Corollary 6.12 (Theorem 2.3, Lifting Lemma)**.** *Given any objects* $X \in \mathcal{C}$, $Y \in \mathcal{C}$, *and* $x \in FX$, $y \in FY$, *if* $lFix(x) \leq lFix(y)$ *in* $lAut(F)$, *then there exist a unique arrow* $X \xrightarrow{f} Y$ *in* $\mathcal{C}$ *such that* $F(f)(x) = y$.

Proof. Notice that the Galois group $lFix(x)$ for the action of $lAut(F)$ on FX is given by $lFix(x) = \#[(X, < x\,|\,x >)]$ (see 7.2). Thus, clearly, this statement is the particular case of 6.11, when $x_0 = x_1$ and $y_0 = y_1$. $\square$

7. PRELIMINARIES ON THE CLASSIFYING TOPOS OF A LOCALIC GROUP

Given a set X, by the construction in proposition 3.3, the following equations hold in the local $lAut(X)$ (recall that we abuse the notation and omit to indicate the associate sheaf morphism):

$$[<z\,|\,x>,\ <z\,|\,y>] = 0\,,\quad [<x\,|\,z>,\ <y\,|\,z>] = 0\quad (each\ x \neq y,\ z)$$

$$\bigvee_x [<x\,|\,z>] = 1\,,\quad \bigvee_x [<z\,|\,x>] = 1\quad (each\ z)$$

Recall also that a *morphism of localic groups* $H \xrightarrow{\varphi} G$ is a continuous map such that $m^*\varphi^* = (\varphi^* \otimes \varphi^*)\,m^*$ (where m denotes the multiplication in the two structures).

Definition 7.1. Given a localic group G and a set X, an *action* of G on X is a continuous morphism of localic groups $G \xrightarrow{\mu} lAut(X)$. It is completely determined by the value of its inverse image on the generators, $X \times X \xrightarrow{\mu^*} G$. We say that the action is *transitive* when for all $x \in X$, $y \in X$, $\mu^*[< x\,|\,y >] \neq 0$.

Definition 7.2. Given a localic group G acting on a set X, and element $x \in X$, the open subgroup of G, described informally as $\{g \in G \mid gx = x\}$, is defined to be the object $lFix(x) = \mu^*[< x\,|\,x >]$ in the locale G.

Given a localic group G, a *G-set* is a set furnished with an action of G. Given two G-sets X, Y, $X \times X \xrightarrow{\mu^*} G$, $Y \times Y \xrightarrow{\mu^*} G$, a morphism of G-sets is a function $X \xrightarrow{f} Y$ such that $\mu^*[< x\,|\,y >] \leq \mu^*[< f(x)\,|\,f(y) >]$. This defines a category $\mathcal{B}G$

furnished with an underline set functor $\mathcal{B}G \xrightarrow{|\,|} \mathcal{E}ns$ into the category of sets. We shall denote $t\mathcal{B}G$ the full subcategory of non empty transitive G-sets.

It is easy to check the following (consider 4.7 and 4.8):

Proposition 7.3. *Let F be the underline set functor $\mathcal{B}G \xrightarrow{|\,|} \mathcal{E}ns$. The map given by $[(X, <x_0\,|\,x_1>)] \longmapsto \mu^*[<x_0\,|\,x_1>]$ determines (the inverse image of) a morphism of localic groups $G \to lAut(F)$.*

Proposition 7.4. *All morphisms $X \xrightarrow{f} Y$ between non empty transitive G-sets are surjective functions of the underline sets.*

Proof. We shall see that $\forall\, y \in Y \ \ \exists\, x \in X \ \mid\ f(x) = y$.
  Take any $x_0 \in X$ and let $y_0 = f(x_0)$. Then:

$$1 \;=\; \bigvee_x \mu^*[<x_0\,|\,x>] \;\leq\; \bigvee_x \mu^*[<y_0\,|\,f(x)>]$$

Taking the infimum against $\mu^*[<y_0\,|\,y>]$,

$$0 \;\neq\; \mu^*[<y_0\,|\,y>] \;\leq\; \bigvee_x \mu^*[<y_0\,|\,y>,\ <y_0\,|\,f(x)>]$$

The terms in the supremum are equal to 0 except if $y = f(x)$. This finishes the proof. $\qquad\square$

Proposition 7.5. *Given a localic group acting on set, $G \xrightarrow{\mu} lAut(X)$, $X \times X \xrightarrow{\mu^*} G$, the relation $x \sim y \ \Leftrightarrow\ \mu^*([<x\,|\,y>]) \neq 0$ is an equivalence relation on X, and G acts transitively on each equivalence class.*

Proof. Assume $\mu^*[<x|z>] \neq 0$ and $\mu^*[<z|y>] \neq 0$. The multiplication m of $lAut(X)$ is given by

$$m^*([<x\,|\,y>]) \;=\; \bigvee_z [<x\,|\,z>] \otimes [<z\,|\,y>]$$

Since μ^* is a morphism of groups as well as of locales,

$$m^*\mu^*[<x|y>] \;=\; (\mu^* \otimes \mu^*)\, m^*[<x|y>] \;=\; \bigvee_z \mu^*[<x|z>] \otimes \mu^*[<z|y>]$$

It follows that $m^*\mu^*([<x\,|\,y>]) \neq 0$. Thus $\mu^*([<x\,|\,z>]) \neq 0$. The second assertion is obvious. $\qquad\square$

Given an element $x_0 \in G$, the *connected component* of x_0 is the transitive G-set with underline set $\{x \in X \mid \mu^*([<x\,|\,x_0>]) \neq 0\}$.

The coproduct of G-sets is just the disjoint union furnished with the obvious action ($\mu^*[<x|y>] = 0$ if x and y are in different components). In this way, every G-set is the coproduct in $\mathcal{B}G$ of transitive G-sets. With this it is clear that it follows from 7.5 that *a G-set is a connected object in $\mathcal{B}G$ if and only if the action is transitive.*

Proposition 7.6. *The diagram of the underline set functor $t\mathcal{B}G \xrightarrow{|\,|} \mathcal{E}ns$ (from the category of non empty transitive G-sets) is a cofiltered poset. That is:*

1) *Given morphisms of transitive G sets,* $X \overset{t}{\underset{s}{\rightrightarrows}} Y$ *and* $x_0 \in X$ *such that* $s(x_0) = t(x_0)$, *then* $s = t$.

2) *Given two transitive G-sets* X, Y, *and elements* $x \in X$, $y \in Y$, *there exists a transitive G-set M, an element $m \in M$, and morphisms of G-sets* $M \overset{s}{\longrightarrow} X$, $M \overset{t}{\longrightarrow} Y$, *such that* $s(m) = x$, $t(m) = y$.

Proof. 1) Let $y_0 = s(x_0) = t(x_0)$, and let x be any element in X. Since $0 \neq \mu^*([< x_0 \mid x >]$ it follows that $0 \neq \mu^*[< y_0 \mid s(x) >, \ < y_0 \mid t(x) >]$. Thus it must be $s(x) = t(x)$

2) Take the connected component of (x, y) in the product $X \times Y$ and the two projections (the action in the product is given by $\mu^*[< (x, y) \mid (x', y') >] = \mu^*[< x \mid x' >] \wedge \mu^*[< y \mid y' >]$). $\qquad\square$

Proposition 7.7. *All morphisms* $X \overset{f}{\longrightarrow} Y$ *between non empty transitive G-sets are strict epimorphisms in* $t\mathcal{B}G$.

Proof. Let $X \overset{g}{\longrightarrow} Z$ be such that $Ker_f \subset Ker_g$ (see 6.1).

We shall see first that $Ker_{|f|} \subset Ker_{|g|}$ taken in $\mathcal{E}ns$. Let $x \in X$, $y \in X$ be such that $f(x) = f(y)$. Take $M, m \in M$, s and t as in 7.6,2). Then $fs(m) = ft(m)$, and thus $s = t$. By assumption it follows $gs = gt$, thus $g(x) = g(y)$.

From this, since f is surjective (7.4), it follows there exists a function $Y \overset{h}{\longrightarrow} Z$ such that $hf = g$. It remains to see that h is a morphism of G-sets. We do this now.

Let y_0, y_1 be any two points in Y. Take $x_0 \in X$, $f(x_0) = y_0$. We have $\mu^*[< y_0 \mid y_1 >] \wedge \mu^*[< x_0 \mid x >] \ \leq \ \mu^*[< y_0 \mid y_1 >, \ < y_0 \mid f(x) >]$, which equals 0 unless $f(x) = y_1$. With this:

$$\mu^*[< y_0 \mid y_1 >] \ = \ \bigvee_x \mu^*[< y_0 \mid y_1 >] \wedge \mu^*[< x_0 \mid x >] \ =$$

$$\bigvee_{f(x)=y_0} \mu^*[< y_0 \mid y_1 >] \wedge \mu^*[< x_0 \mid x >] \ \leq \ \bigvee_{f(x)=y_0} \mu^*[< x_0 \mid x >] \ \leq$$

$$\bigvee_{f(x)=y_0} \mu^*[< g(x_0) \mid g(x) >] \ = \ \mu^*[< h(y_0) \mid h(y_1) >]$$

$$\square$$

Clearly, by definition, given a morphism of G-sets $X \overset{h}{\longrightarrow} Y$, if $x_0 \in X$, and $y_0 = h(x_0)$, we have $lFix(x_0) \leq lFix(y_0)$ in G. The reverse implication also holds, which means that transitive G-set are in a sense quotients of G.

Proposition 7.8. *Let X be any transitive G-set, $x_0 \in X$. Given any G-set Y, $y_0 \in Y$, such that $lFix(x_0) \leq lFix(y_0)$ in G, there exists a unique morphism* $X \overset{h}{\longrightarrow} Y$ *such that* $h(x_0) = y_0$.

Proof. Take $M, m_0 \in M$, $M \overset{f}{\longrightarrow} X$ and $M \overset{g}{\longrightarrow} Y$, $f(m_0) = x_0$, $g(m_0) = y_0$ (7.6,2). To prove the statement it is enough to show that

$Ker_f \subset Ker_g$ (7.7). First we prove the following implication:

$$1) \quad \forall m \in M, \; f(m) = x_0 \; \Rightarrow \; g(m) = y_0$$

Assume $f(m) = x_0$. Then, $\mu^*[< m_0 \mid m >] \leq \mu^*[< y_0 \mid g(m) >]$, and, $\mu^*[< m_0 \mid m >] \leq \mu^*[< x_0 \mid x_0 >] \leq \mu^*[< y_0 \mid y_0 >]$. Thus $0 \leq \mu^*[< y_0 \mid y_0 >, \; < y_0 \mid g(m) >]$. It follows $g(m) = y_0$.

With this, now we prove $Ker_f \subset Ker_g$. Let $Z \xrightarrow[\;\;t\;\;]{\;\;s\;\;} Y$ be in Ker_f, that is, $fs = ft$. Take z_0 such that $fs(z_0) = ft(z_0) = x_0$ (7.4). Then, for any $z \in Z$,

$$0 \; \leq \; \mu^*[< z \mid z_0 >] \; \leq \; \mu^*[< gs(z) \mid gs(z_0) >] \wedge \mu^*[< gt(z) \mid gt(z_0) >]$$

$$\leq \mu^*[< gs(z) \mid y_0 >, \; < gt(z) \mid y_0 >] \,,$$

the last inequality justified by 1). It follows that $gs(z) = gt(z)$, thus $gs = gt$. This finishes the proof. $\qquad\square$

Corollary 7.9. *If the localic group G is small (meaning it has only a set of objects), then the category $t\mathcal{B}G$ is also small.*

Proof. Let F be the underline set functor $t\mathcal{B}G \to \mathcal{E}ns$. Then the map $\Gamma_F \to G$ given by $(X, x_0) \longmapsto \mu^*[< x_0 \mid x_0 >]$ creates (thus also reflects) isomorphisms (compare with 7.3). $\qquad\square$

8. Characterization of the classifying topos of a localic group

In this section we characterize the category $\mathcal{B}G$ of G-sets in terms of the theory of topoi. That is, we prove Theorem B in the introduction. We shall see how this characterization follows in an straightforward manner from theorems 2.3 and 2.2.

First recall that a *connected atomic topos* is a connected, locally connected and boolean topos. The reference for atomic topoi and atomic sites is [2]. For connected and locally connected topoi see [1], Expose IV, 2.7.5, 4.3.5, 7.6 and 8.7.

We have:

Proposition 8.1. *Let $\mathcal{C}$ be a category and $F : \mathcal{C} \longrightarrow \mathcal{E}ns$ be a functor as in 2.1, i) and iii). Then the canonical (in this case atomic) topology defines an atomic site with a point. If $\mathcal{C}$ is small, the topos of sheaves $\mathcal{C}^\sim$ is an atomic topos with a point (see [2]). This topos is connected if and only if condition ii) holds. Any connected atomic topos with a point can be presented in this way.*

Proposition 8.2. *The category $t\mathcal{B}G$ of transitive G-sets satisfies 2.1. If G is small, $\mathcal{B}G$ is an atomic topos with a point, with inverse image given by the underline set ($\mathcal{B}G$ is the topos of sheaves for the canonical topology on $t\mathcal{B}G$).*

Proof. The first assertion is given by 7.7 and 7.4. The second follows from 7.5 and 7.9.   □

Consider now any category $\mathcal{C}$ and any set valued functor $\mathcal{C} \xrightarrow{F} \mathcal{E}ns$. Then, proposition 4.8 shows that F lifts into a functor, that we denote μF, $\mathcal{C} \xrightarrow{\mu F} \mathcal{B}G$, for $G = lAut(F)$. We have:

Theorem 8.3. *Let $\mathcal{C}$ and $\mathcal{C} \xrightarrow{F} \mathcal{E}ns$ be as in 2.1. Then the functor μF lands into $t\mathcal{B}G$, $\mathcal{C} \xrightarrow{\mu F} t\mathcal{B}G$. If $\mathcal{C}$ is small, then G is small, and μF induces an equivalence of categories $\mathcal{C}^{\sim} \xrightarrow{\cong} \mathcal{B}G$ between the topoi of sheaves for the canonical topology on $\mathcal{C}$ and the classifying topos $\mathcal{B}G$.*

Proof. Theorem 2.2 just says that μF lands into $t\mathcal{B}G$. We shall prove:
  1) The functor μF (which is faithful since F is, see 6.3) is also full.
  2) Given any transitive G-set S, there exists $X \in \mathcal{C}$ and an strict epimorphism $\mu FX \to S$ in $t\mathcal{B}G$.
  proof of 1). This is just the meaning of Theorem 2.3. Given a morphism of G-sets $\mu FX \xrightarrow{f} \mu FY$, choose any $x_0 \in FX$, and let $y_0 = f(x_0)$. By definition $lFix(x_0) \le lFix(y_0)$ in G.
  proof of 2). Choose any $s_0 \in S$. Consider $lFix(s_0) \in G$. Clearly $e \in lFix(s_0)$. Then, by 4.9, and the construction of $lAut(F)$ (4.7), since Γ_F is cofiltered, it follows that there is $X \in \mathcal{C}$ and $x_0 \in FX$, such that $lFix(x_0) = \#[(X, <x_0 \,|\, x_0>)] \le lFix(s_0)$. The proof finishes then by 7.7 and 7.8.
  The theorem follows from 1) and 2) by the comparison lemma ([1], Expose III, 4.).

                                                                        □

We can now easily establish Theorem B.

Theorem 8.4. *A topos $\mathcal{E}$ with a point $\mathcal{E}ns \xrightarrow{p} \mathcal{E}$, $p^* = F$, is connected atomic if and only if it is the classifying topos $\mathcal{B}G$ of a localic group G, and this group can be taken to be $lAut(F) = lAut(p)^{op}$.*

Proof. From 8.1 it follows that the easy direction on this equivalence is given by 8.2, and the hard direction by 8.3.   □

References

[1] Artin M, Grothendieck A, Verdier J., *SGA 4 , (1963-64)*, Lecture Notes in Mathematics 269 and 270, Springer, (1972).
[2] Barr M, Diaconescu R, *Atomic Toposes*, Journal of Pure and Applied Algebra 17 (1980).
[3] Edwards H. M., *Galois Theory*, Graduate Texts in Mathematics 101, Springer (1984).
[4] Joyal A., Tierney M., *An extension of the Galois Theory of Grothendieck*, Memoirs of the American Mathematical Society 151 (1984).
[5] Wraith G., *Localic Groups*, Cahiers de Top. et Geom. Diff. Vol XXII-1 (1981).